**Statement for the Record**

**J. Michael Hickey**

**Vice President - Government Affairs**
**National Security Policy**

**Before the**

**Committee on Homeland Security**
**Subcommittee on Emergency Communications, Preparedness and Response**

**U.S. House of Representatives**

# "Leveraging the Private Sector to Strengthen Emergency Preparedness and Response"

**July 19, 2007**

**10:00 AM, Cannon House Office Building, CHOB-311**

**Introduction:**
My name is Mike Hickey. I am here today representing Verizon Corporation as Vice President of Government Affairs for National Security Policy. In addition to my responsibilities at Verizon, I currently serve as Chair for the Communications Sector Coordinating Council, as Vice Chair of the Internet Security Alliance and as an active member of the US Chamber of Commerce Homeland Security Task Force. Of these organizations, the US Chamber of Commerce is unique in that it represents the breadth and diversity of American commerce. And since 2003, it has advocated for strong business engagement in matters relating to homeland security and emergency preparedness.

My comments will address efforts that business has made to strengthen this country's economic and homeland security, where it has partnered successfully with government and how we might collectively tighten our efforts to ensure greater effectiveness in the future.

**I. Tiered Approach to Operational Readiness:**
Effective industry and government collaboration starts with the actions of individual organizations. Where the private sector owns and operates 85-90% of this country's critical infrastructure, corporations like Verizon must dedicate the operations experience, resources and oversight necessary to be as self-aware and self-reliant as possible. We are obligated to our shareowners and customers to take the necessary steps to secure our physical, cyber and human assets from disruption or attack. We must continue to cooperate with peer companies and to support communications sector mutual aid obligations. We must also proactively address our interdependencies with other sectors to ensure continuity of operations in time of crisis. And we must continue to work with government agencies at the Federal, State, regional and local levels to support appropriate security and emergency preparedness initiatives.

**Strength from Within:**
Verizon's commitment to national security and emergency preparedness – grounded in corporate policy, sound business practice and hands-on experience – is long-standing and growing.

Verizon has an established policy which requires every business unit to maintain a high level of preparedness, consistent with the company's unique role in furnishing critical telecommunications and information services to the Federal government, to State and local government, to many of this country's largest corporations and to the general public. The policy requires business units to establish and maintain continuity of operations and management plans which may be used to maintain and restore critical services under conditions ranging from local emergencies to widespread disasters.

Where individual business units have an obligation to create, manage, certify and test business continuity programs at the ground level, a governance structure has been implemented to ensure corporate-wide effectiveness in operational and security practice.

In order to ensure the continuity of its own operations and to meet the requirements of its critical customers in time of crisis, Verizon has:

- Designed, built and managed network facilities that are robust and resilient;
- Embraced "best practice" business methods and security procedures;
- Created and tested business continuity and emergency preparedness programs that have served the corporation and its customers in times of stress;
- Responded successfully to a wide range of crises; and,
- Provided leadership strength to industry and government organizations dedicated to national security and emergency preparedness.

**Sector Leadership and Collaboration:**
Verizon, and its peer companies within the Communications Sector, have a long history of cooperation in time of crisis. This history distinguishes the Communications Sector from most other critical sectors identified in the National Infrastructure Protection Plan. The sector personifies cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. The Sector Specific Agency for the Communications Sector is the National Communications System (NCS) within the Department of Homeland Security's National Cyber Security and Communications Division. The Federal Communications Commission is emerging as another important government partner for the sector.

Historically members of the Communications Sector have been regulated at State and Federal levels. They have partnered closely among themselves and with the Federal government since the establishment of the National Coordinating Center for Telecommunications. In 1982, telecommunications industry and Federal Government officials identified the need for a joint mechanism to coordinate the initiation and restoration of national security and emergency preparedness telecommunications services. In 1984, Executive Order 12472 broadened the NS/EP role of the National Communications System and created the National Coordinating Center for telecommunications as a central public-private sector organization to coordinate response to emergency communications situations.

The use of mutual aid agreements between industry signatories has afforded Communications Sector businesses with access to expanded operational capacity and resources to speed recovery. These mutual aid agreements worked very effectively over the years, in responding to ice storms and earthquakes and in the aftermath of the hurricanes that devastated vast numbers of Gulf Coast communities in 2004 and 2005.

**Cross-Sector Relationships:**
Verizon recognizes its critical operational reliance on other business sectors such as electric and water and has established the necessary vendor relationships to meet both normal and extraordinary continuity of business requirements. In turn, all critical sectors are heavily reliant on the Communications Sector to support continuity of their operations.

The complexity of cross sector independencies was recognized in the 2006 National Infrastructure Protection Plan, resulting from Homeland Security Presidential Directive 7. HSPD-7 focused on the identification, prioritization and protection of the nation's critical assets. It required the development of the National Infrastructure Protection Plan (NIPP) and corresponding Sector Specific Plans.

Perhaps most significantly, the NIPP encouraged the establishment of sector coordinating councils. In so doing, it brought greater sector diversity to the table and significantly advanced the institutional capacity of sectors to formally and proactively address cross-sector dependencies. As an example, the Communications and Information Technology Coordinating Councils operate independently, but in close alignment with each other.

Currently, the Communications, IT and Financial Services Sectors are working with the National Communications System to review the potential consequences of predicted, extraordinarily high telecommuting levels on network access resulting from social distancing protocols during a Pandemic Influenza. The outcomes of this review should be useful to government and business planners and to the public at large. This typifies the utility of these newly established sector coordinating councils and their ability to plan and coordinate across sector bounds.

**Partnerships with Government:**
Today's all-hazards threat environment poses significant leadership and resource challenges for the private sector, which as highlighted earlier, owns and operates the vast majority of this country's critical assets. Operating successfully in this environment includes being prepared to respond to threats that are both natural and man-made. With ever-changing technology and marketplace demands, business must remain agile in order to adjust business practices and technology solutions to protect its most critical assets.

Government-imposed solutions may hinder the ability of business to adapt and respond effectively to the changing threat environment. So it becomes critical for business and government to work collaboratively towards solutions that are meaningful, adaptable and sustainable. The voluntary development of and compliance with "best/sound practice" approaches to physical and cyber security is a model that is time tested. It is illustrated through the work of the Federal Communications Commission Network Reliability and Interoperability Council. The NRIC is a successor to the National Reliability Council, first established in 1992. Through the work of seven successive councils, subject matter experts from business and government have come together to address network reliability and interoperability issues of concern, develop best/sound practices and encourage voluntary adoption.

The National Security Telecommunications Advisory Committee, established in 1982, provides another relevant example of how the private sector can assist and help direct government decisions around national security and emergency preparedness communications. This advisory committee to the President brings together 30 industry chief executives representing major telecommunications companies, network providers, information technology companies, finance and aerospace businesses. NSTAC provides industry-based advice and expertise to the President on a wide range of telecommunications issues regarding communications, information security, information assurance, critical infrastructure protection and other national security and emergency preparedness issues.

IN SUMMARY, this tiered approach to business continuity and emergency preparedness – one that builds on internal readiness and reliance on effective business and industry partnerships, continues to meet Verizon's operational and customer requirements. It has also advanced this country's emergency preparedness and response capabilities.

**II. Broader Private Sector Initiatives:**
Outside of the Communications Sector, numerous trade associations and national organizations such as the US Chamber of Commerce and Business Executives for National Security (BENS) have advanced emergency preparedness and response initiatives with government. These organizations provide companies like Verizon an opportunity to confer with industry and government leaders, share best/sound practices, better understand cross-sector complexities and train and exercise with industry and government partners.

The US Chamber of Commerce Homeland Security Division works to ensure that the Department of Homeland Security and Congress effectively strike the right balance between homeland security and the openness and mobility critical to the nation's economy. The Division is comprised of 170 representatives from 135 member companies, associations, and State and local chambers. It has advanced the following initiatives:

- ***Ready Business* Summits:** Worked with DHS to engage small and mid-cap companies to ensure pro-active preparation for all types of emergencies. Currently hosting a series of *Ready Business* Summits around the country in partnership with State and local chambers to broaden awareness of DHS *Ready Business* initiatives, tools and resources available for emergency planning.
- **Pandemic Preparedness:** Convened a pandemic planning work group (45 companies) to address pandemic policy issues and to provide private sector input into government strategies. Currently hosting regional business pandemic preparedness roundtables with DHS and the Centers for Disease Control and Prevention (CDC) to discuss the role of the business in pandemic planning and response. Planning legal and HR-related pandemic seminars in conjunction with DHS.
- **Critical Infrastructure Protection/Information Sharing:** Launched a project with DHS to fully engage the private sector with State homeland security directors. This initiative is intended to institutionalize private sector participation in State fusion centers and homeland security departments and in all aspects of planning, training and exercises.
- **Strategic Engagement with DHS:** Currently reviewing the Private Sector Annex of the National Response Plan which addresses private sector coordination and integration. Invited to participate in the TOPOFF 4 exercise in October. Connecting Chamber members with FEMA to help strengthen the FEMA disaster logistics supply chain.
- **Public-Private Partnership with the Intelligence Community:** Scheduling briefings with the Office of the Director of National Intelligence (ODNI) on issues of mutual, long-term strategic interest, but not limited to: China; global energy market challenges; insider threats from terrorism; India and failing states and the erosion of national sovereignty.
- **Supply Chain Security:** Helped advance port and supply chain security legislation (the SAFE Port Act). Will co-host, together with BUSINESS EUROPE, a September transatlantic security summit focused on shared security challenges such as supply chain security. The summit will feature high-level participation by government and business leaders in the EU and the U.S.
- **Iraq Sourcing Initiative:** Partnering with the Institute for Defense and Business to support the DOD Task Force to Improve Business and Stability Operations in Iraq.
- **National Guard and Reserve:** Worked with the Commission on the National Guard and Reserves to help provide businesses the needed predictability to plan for when and how long their employers may be called up. Coordinated with the Employer Support of the Guard and Reserve (ESGR) Defense Advisory Board to strengthen the compact between employers and the Reserve Component.

IN SUMMARY, these US Chamber of Commerce initiatives provide just a sampling of the work that is underway by the private sector to strengthen this country's emergency preparedness and response capabilities. Business Executives for National Security also provides effective cross-sector forums for advancement of leading edge approaches to these critical issues.

What cannot be underestimated by policymakers is the enormous amount of private sector resources that are being devoted to finding solutions – with government partners – designed to achieve greater effectiveness in our country's security and response programs. The private sector has demonstrated its willingness to commit significant financial resources and expertise to strengthen critical business practices. At the same time, it has dedicated time and energy and expertise to its work with government partners to address emerging legal and regulatory considerations. A key business concern is to not become encumbered by unnecessary oversight and controls that may restrain, rather than encourage, innovative solutions to emergency preparedness and response.

**III. Working Towards Greater Effectiveness:** Almost six years have passed since 9-11. During this time, much has been accomplished by private and Government sectors in achieving more effective emergency preparedness and response for our country and its citizens. Yet significant work remains. In the months ahead, it will become even more essential for partners to carefully prioritize initiatives, ensure that real partnership cooperation and inclusion is achieved and that critical pieces of "unfinished business" are addressed.

**Interagency and Private Sector Cooperation at the Regional and Local Level:** In Homeland Security Presidential Directive 5 (HSPD-5), the President directed the establishment of the National Incident Management System (NIMS) and the National Response Plan (NRP) to align Federal coordination capabilities and resources into a unified, self-disciplined and all-hazards approach to domestic incident management. The basic premise of the NRP is that incidents are generally handled at the lowest jurisdictional level possible.

In recent weeks, a ten-day ESF-2 (the Communications Support Function annex to the National Response Plan) exercise, training program and technology demonstration took place in New Orleans. It was designed to bring Federal agency personnel and State, regional and local emergency response personnel together to exercise, train and become better acquainted with agency roles, responsibilities and resources. It also brought in the private sector to help plan and participate in an active and meaningful way.

The program mustered personnel and resources from agencies such as the National Communications System, the Federal Communications Commission's Homeland Security Bureau, FEMA and GAO. Other agencies had more limited representation. The initiative achieved success from many standpoints – especially in bringing critical Communications Sector representatives together to establish relationships and to clarify roles and responsibilities.

This approach is crucial – especially as Federal agency personnel work to establish a lasting presence at the local and regional level. The private sector must be viewed as intrinsic to such training and exercise programs, not as an understudy. The private sector resources and expertise brought to bear in the New Orleans exercise made that program more meaningful to all.

And the presence of key federal agencies encouraged a better understanding of how Joint Field Office programs and leadership can work together in time of crisis.

From a broader perspective, meaningful business and government partnerships are created not just through dialogue and planning, but by testing operational readiness and exercising together. The early insertion of private sector ideas and expertise in training exercises brings greater meaning to such programs – whether at the local and regional level or in the development of national exercises such as TOPOFF 4.

**Coordinated Private Sector Outreach:** The Department of Homeland Security has been well-served by both its Private Sector Liaison office and by the Infrastructure Protection Partnership and Outreach office. These offices have been visible and accessible, while being proactive in bridging the private sector with the work of the Department on issues ranging from information sharing to pandemic planning. At the same time, they have worked with limited resources on an unlimited stage. As a result, their combined impact has been educational in nature, rather than being operationally focused.

As additional resources are devoted to standing up Department programs at the regional level in support of Joint Field Office requirements, agencies such as FEMA must create stronger private

sector outreach and coordination capacity that will encourage and sustain private sector participation over the long term. Such efforts will yield stronger private sector interest and resources that can be leveraged in agency emergency preparedness and response programs.

I am happy to report that FEMA Administrator, David Paulison and his regional administrators are taking this public/private partnership seriously. As an example, senior leaders from Verizon's regional offices have recently met with the senior leadership from the FEMA Region 1 (Boston) and FEMA Region 6 (Denton, TX) offices in an effort to further develop already-existing disaster preparedness relationships. The goal of these meetings has been for FEMA to better understand Verizon's capabilities in time of crisis so that the public sector has a better knowledge of what the private sector has to offer by way of response, recovery and restoration capabilities. Likewise, Verizon has been able to more clearly understand FEMA's operational needs, as a result of these discussions.

**Renewed Focus on "Unfinished Business":** Much has been accomplished by business and government partners to address emergency preparedness and response issues raised by actual events. In some instances though, jurisdictions have established localized "model" programs to improve response capacity that are not adopted in neighboring jurisdictions. In other instances, broader solutions have been developed that have failed to garner the necessary multi-jurisdiction to make them effective.

**Access and Credentialing:** Priority access to disaster sites is critical for private sector emergency responders to enable them to recover, repair, and reconstitute critical communications infrastructure essential for NS/EP communications. There is a provision in the WARN Act designating telecommunications companies as "essential service providers," which entitles them to unimpeded access to disaster sites "to the greatest extent practicable."

However, because such access will only be allowed to the greatest extent possible, government authorities have the discretion to deny access when they determine it is not "practicable." It is unclear whether such discretion can be challenged, and this provision is not a panacea to the access problems exposed in the aftermath of Katrina. This priority issue requires additional work effort for both business and government partners. Moreover, as the Katrina experience indicated, telecommunications and other utility providers need resources as well as access to effectively restore services. Additional changes to the Stafford Act are needed to correct this.

Credentialing is a related issue that requires additional attention. At the Federal level, DHS has developed a national identification (ID) card system that can verify identities of responders who appear at an incident scene. The Department's ID card effort is part of a two-pronged solution for credentialing that also includes defining and creating categories of emergency responders, including firefighters, hazardous materials teams, and private sector workers. While this is viewed as a long term solution to emergency credentialing, state jurisdictions are developing localized approaches. Business and government partners must press ahead now to achieve cross-jurisdictional, short-term solutions.
**Wireless Shutdown and Restoration Protocols:** Given the rise in terrorist activity in the past few years, and an incomplete understanding of the technology involved in such activities, certain government authorities have, in certain circumstances, wondered whether the need may arise to disrupt or disable access to cellular service within a particular geographic area in the name of public safety. Because a disruption of even a portion of a cellular network would impact the public, the National Communications

System (NCS) has taken on the role of coordinating any actions leading up to and implementing such decisions. Business and government partners must now educate and enlist the support of local jurisdictions to implement the protocols.

**Better Coordination in Crises:** The Katrina experience demonstrated the need for improved coordination, cooperation and communication at and among all levels of government. Recent administrative and legislative reorganizations at DHS have moved functions and missions across components and created new structures and offices (for example the Office of Emergency Communications, enhanced role of FEMA etc.). It remains to be seen if all these changes will be effectively and efficiently implemented by the time the next disaster strikes.

IN SUMMARY, private and government sector partnerships in emergency preparedness and response remain a work in progress. Although stronger in quality and scope, much work remains. The real value of progress made to date will be measured by the collective response to this country's next major natural disaster or terrorist attack. If our emergency preparedness and response yields more favorable results for the security of our citizenry and our critical assets we will know that we have been heading in the right direction.

At Verizon, we will continue to fine tune our business continuity practices, our investments and our internal protocols to build upon past successes. And yet our ultimate success as a communications provider and corporate citizen will rely on the success of our external relationships with sector peers, cross-sector allies and government partners. We need to press ahead to better target priorities, establish trusted relationships and address gaps.